Claims

1. A method of installing a network device in a packet-based data communication network and checking the authenticity of the installation, comprising the steps of:

(a) communicating identification information of the device to a management system;

(b) installing said device;

(c) obtaining from a protocol address administrator a protocol address for said device;

(d) sending a communication from the device to the management system;

(e) conducting a key agreement protocol exchange between said device and said management system to establish a set of encryption keys;

(f) using said set of encryption keys to provide mutual authentication by said device and said management system;

(g) associating, within said management system, the time of said communication in step (d) with said identification information and the protocol address of the device;

(h) communicating from said management system to said administrator a message including said identification information, said protocol address and said time.

2. A method according to claim 1 wherein, after said step (g) said management system produces further encryption keys for subsequent communications between said management system and said device.

3. A method according to claim 2 wherein said management system sends to said device a reset key enabling reiteration of a key agreement protocol exchange corresponding to step (e).

4. A method according to claim 1 and further comprising periodically sweeping through all addresses available to said management system and comparing said addresses with addresses of devices compiled by means of step (f).

5. A method according to claim 1 wherein said identification information includes a revealed encryption key.

6. A method according to claim 5 wherein said device has stored therein a manufactured encryption key which is related to said revealed encryption key.